Abstract

Apparatus for use by a first party for key management for secure communication with a second party, said key management being to provide at each party, simultaneously remotely, identical keys for said secure communication without transferring said keys over any communication link, the apparatus comprising: a datastream extractor, for obtaining from data exchanged between said parties a bitstream, a random selector for selecting, from said bitstream, a series of bits in accordance with a randomization seeded by said data exchanged between said parties, a key generator for generating a key for encryption/decryption based on said series of bits, thereby to manage key generation in a manner repeatable at said parties.